Una generalización de la función aritmética $g(n) = \prod_{j=1}^{n} (j, n)$ y algunas de sus aplicaciones

Francisco Niño Rojas

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá

2010

Una generalización de la función aritmética $g(n) = \prod_{j=1}^{n} (j, n)$ y algunas de sus aplicaciones

Francisco Niño Rojas

Trabajo final presentado como
requisito parcial para optar al título de
Magister en Matemáticas

Director
Víctor Samuel Albis González

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá
2010

Contenido

Introducción

En este trabajo estudiaremos la función definida por:

$$g(n;h) := \prod_{j=1}^{n} h((j,n)), \tag{0.1}$$

donde $(j,n) := mcd(j,n)$ es el máximo común divisor de j y n y $h(x)$ es una función aritmética. Para $e(x) := x$ denotamos $g(n) = g(n;e)$ y definimos:

$$g(n) := \prod_{j=1}^{n} (j,n), \tag{0.2}$$

lo que convierte a (0.1) en una generalización de (0.2).

En el segundo capítulo estudiaremos algunas evaluaciones, identidades y propiedades de las funciones $g(n;h)$, $g(n)$ y $f(n;h) := g(n;h)^{\frac{1}{n}}$.

Posteriormente evaluaremos (0.1) en términos de series de Dirichlet que conducen a varias identidades que involucran la función zeta de Riemann y la serie $\sum_{n=1}^{\infty} \frac{\log[h(n)]}{n^s}$, además mostraremos algunos comportamientos asintóticos para $g(n;h)$ y para el caso especial $g(n)$.

Por último trataremos algunas aplicaciones relacionadas con esta función; por ejemplo:

a) Para un entero positivo n, encontraremos el número de soluciones distintas modulo n de la congruencia $x^{n-1} \equiv 1 (mod\, n)$.

   Si n es un entero compuesto impar cada solución coincide con un número b tal que n sea un seudoprimo con base b. En este caso encontraremos el número de enteros b tales que n sea un seudoprimo con base b [8].

b) Otra aplicación surge en el estudio del número de puntos reticulares sobre rectas en el plano ([1], [4]); si consideramos dos puntos P y Q sobre el plano, encontramos el número de puntos reticulares que hay sobre el segmento $\overline{PQ}$. Si damos varios segmentos sobre el plano, es posible encontrar el número de caminos que que se pueden trazar entre los puntos reticulares.

Capítulo 1

Preliminares

Este capítulo esta dedicado a recordar algunos conceptos y resultados básicos que serán de utilidad a lo largo de este trabajo.

Definición 1.1. ***Series de Dirichlet***

Llamamos series de Dirichlet a aquellas series de la forma

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

en donde $f(n)$ *es una función aritmética y* $s \in \mathbb{C}$.

Considerando $s = \sigma + it$ podemos abordar un caso especial de una serie de Dirichlet conocido como la función zeta de Riemann.

Definición 1.2. ***Función zeta de Riemann***

La función zeta de Riemann se define

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad si \quad \sigma > 1.$$

El teorema siguiente nos permite calcular las abscisas de convergencia de las series de Dirichlet que nos van a aparecer en la práctica.

Antes veamos la siguiente definición:

Definición 1.3. ***Abscisa de convergencia absoluta***

Se llama abscisa de convergencia absoluta de una serie de Dirichlet al ínfimo σ_a del conjunto de los números reales en los que la serie converge absolutamente.

Teorema 1.4. *Si existe un $M > 0$ tal que $|f(n)| \leq M$ para todo $n \geq 1$, entonces la serie*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

converge absolutamente para $\sigma > 1$, luego $\sigma_a \leq 1$.

Demostración. Si $|f(n)| \leq M$ entonces

$$\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right| \leq M \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} = M\zeta(\sigma)$$

■

Teorema 1.5. ***Productos de Series de Dirichlet***

Dadas dos funciones F(s) y G(s) representadas por dos series de Dirichlet,

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \textit{para} \quad \sigma > a,$$

y

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \quad \textit{para} \quad \sigma > b.$$

Entonces, en el semiplano en el que ambas series convergen absolutamente, tenemos

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s},$$

en donde $h = f * g$ es la función aritmética dada por:

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Demostración. Para todo s en el que ambas series converjan absolutamente tenemos

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \sum_{m=1}^{\infty} \frac{g(m)}{m^s} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{f(n)g(m)}{(mn)^s}.$$

En virtud de la convergencia absoluta podemos multiplicar estas series y reordenar sus términos convenientemente sin que ello altere la suma. Juntamos los términos para los que mn es constante, $mn = k$. Los posibles valores de $k = 1, 2, ...$; luego

$$F(s)G(s) = \sum_{k=1}^{\infty} \left(\sum_{mn=k} f(n)g(m) \right) k^{-s} = \sum_{k=1}^{\infty} \frac{h(k)}{k^s}.$$

En donde $h(k) = \sum_{mn=k} f(n)g(m)$. ■

Definición 1.6. *Si f y g son funciones aritméticas, llamaremos convolución de Dirichlet de f y g a la función aritmética $f * g$ dada por*

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Consideremos el siguiente ejemplo de utilidad en el tercer capítulo.

Ejemplo 1.7. *Hagamos $f(n) = 1$ y $g(n) = \phi(n)$ (Indicatriz de Euler) en el teorema 1.5 Consideremos que la serie $F(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$ para $\sigma > 1$ y que la serie $G(s) = \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}$ converge absolutamente para $\sigma > 2$, ya que $\phi(n) \leq n$. Luego $h(n) = \sum_{d|n} \phi(d) = n$, entonces por el teorema 1.5*

$$F(s)G(s) = \zeta(s) \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \zeta(s-1) \quad si \quad \sigma > 2.$$

Por consiguiente

$$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \quad si \quad \sigma > 2. \tag{1.1}$$

Consideremos un ejemplo de una serie de Dirichlet analítica usado posteriormente.

Ejemplo 1.8. *Para $\sigma > 1$ tenemos*

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}. \tag{1.2}$$

Que se obtiene derivando término a término la serie correspondiente a la función zeta.

Definición 1.9. *Si $g(x) > 0$ para todo $x > a$, escribiremos*

$$f(x) = O(g(x))$$

para indicar que el cociente $f(x)/g(x)$ se halla acotado para $x \geq a$; esto es, existe una constante $M > 0$ tal que

$$|f(x)| \leq Mg(x) \quad \text{para todo} \quad x \geq a.$$

A continuación se presentan algunas formulas asintóticas utilizadas en el estudio de los comportamientos asintóticos de $g(n;h)$ y $g(n)$.
Para las demostraciones de dichas fórmulas necesitaremos del siguiente teorema, cuya demostración esta dada en [3] página 54.

Teorema 1.10. ***Fórmula de sumación de Euler***
Si f posee derivada continua f' en el intervalo $[y, x]$, en donde $0<y<x$, entonces

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])f'(t)dt + f(x)([x]-x) - f(y)([y]-y).$$

Donde $[t]$ designa parte entera de t.

Teorema 1.11. *Para $x \geq 1$ tenemos*

$$\sum_{n\leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right). \tag{1.3}$$

$$\sum_{n\le x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O\left(x^{\alpha}\right) \quad si \quad \alpha \ge 0. \tag{1.4}$$

$$\sum_{n>x} \frac{1}{n^s} = O(x^{1-s}) \quad si \quad s > 1. \tag{1.5}$$

$$\sum_{n\le x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} + O\left(\frac{1}{x}\right). \tag{1.6}$$

Demostración. Para la relación 1.3 consideramos $[x]$ como la parte entera de x y $f(t) = \frac{1}{t}$ en la fórmula de sumación de Euler, y obtenemos

$$\begin{aligned}
\sum_{n\le x} \frac{1}{n} &= \int_1^x \frac{dt}{t} - \int_1^x \frac{t-[t]}{t^2} dt + 1 - \frac{x-[x]}{x} \\
&= \log x - \int_1^x \frac{t-[t]}{t^2} dt + 1 + O\left(\frac{1}{x}\right) \\
&= \log x + 1 - \int_1^{\infty} \frac{t-[t]}{t^2} dt + \int_x^{\infty} \frac{t-[t]}{t^2} dt + O\left(\frac{1}{x}\right).
\end{aligned}$$

La integral impropia $\int_1^{\infty} \frac{t-[t]}{t^2} dt$ existe puesto que está dominada por $\int_1^{\infty} \frac{1}{t^2} dt$. Además,

$$0 \le \int_x^{\infty} \frac{t-[t]}{t^2} dt \le \int_x^{\infty} \frac{1}{t^2} dt = \frac{1}{x}$$

luego la última ecuación conduce a

$$\sum_{n\le x} \frac{1}{n} = \log x + 1 - \int_1^{\infty} \frac{t-[t]}{t^2} dt + O\left(\frac{1}{x}\right).$$

Haciendo $C = 1 - \int_1^{\infty} \frac{t-[t]}{t^2} dt$ tenemos

$$\sum_{n\le x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right).$$

Para demostrar 1.4 utilizamos una vez más la formula de sumación Euler con $f(t) = t^{\alpha}$ para obtener

$$\begin{aligned}
\sum_{n\le x} n^{\alpha} &= \int_1^x t^{\alpha} dt + \alpha \int_1^x t^{\alpha-1}(t-[t]) dt + 1 - (x-[x])x^{\alpha} \\
&= \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O\left(\alpha \int_1^x t^{\alpha-1} dt\right) + O(x^{\alpha})
\end{aligned}$$

$$= \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha}).$$

Para demostrar 1.5 usamos la relación $\sum\limits_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$ si $s > 0, s \neq 1$ (ver prueba en [3] página 56) con $s > 1$ a fin de obtener

$$\sum_{n>x} \frac{1}{n^s} = \zeta(s) - \sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + O(x^{-s}) = O(x^{1-s})$$

ya que $x^{-s} \leq x^{1-s}$. Para probar 1.6 usamos la serie $\sum\limits_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$ (ver [3] página 228) y tenemos

$$\sum_{n\leq x} \frac{\mu(n)}{n^2} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} - \sum_{n>x} \frac{\mu(n)}{n^2}$$
$$= \frac{6}{\pi^2} + O\left(\sum_{n>x} \frac{1}{n^2}\right) = \frac{6}{\pi^2} + O\left(\frac{1}{x}\right)$$

en virtud de 1.5. ■

Las siguientes estimativas serán útiles en el estudio de los comportamientos asintóticos para $g(n;h)$ y $g(n)$.

Teorema 1.12. *Para $x \geq 2$ tenemos*

$$\Phi_0(x) := \sum_{n\leq x} \phi(n) = \frac{x^2}{2\zeta(2)} + O(x\log(x)). \tag{1.7}$$

$$\Phi_1(x) := \sum_{n\leq x} \frac{\phi(n)}{n} = \frac{x}{\zeta(2)} + O(\log(x)). \tag{1.8}$$

Demostración. Para demostrar 1.7 usemos la conocida relación

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

y obtenemos

$$\sum_{n\leq x} \phi(n) = \sum_{n\leq x}\sum_{d|n} \mu(d)\frac{n}{d} = \sum_{\substack{q,d \\ qd\leq x}} \mu(d)q = \sum_{d\leq x} \mu(d) \sum_{q\leq \frac{x}{d}} q.$$

Usando la relación 1.4 con $\alpha = 1$ tenemos

$$\begin{aligned}\sum_{n\leq x}\phi(n) &= \sum_{d\leq x}\mu(d)\left(\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right)\\ &= \frac{1}{2}x^2\sum_{d\leq x}\frac{\mu(d)}{d^2} + O\left(x\sum_{d\leq x}\frac{1}{d}\right).\end{aligned}$$

Por las estimativas 1.3 y 1.6 obtenemos

$$\sum_{n\leq x}\phi(n) = \frac{1}{2}x^2\left(\frac{6}{\pi^2} + O\left(\frac{1}{x}\right)\right) + O(x\log x) = \frac{3}{\pi^2}x^2 + O(x\log x).$$

Haciendo $\zeta(2) = \frac{\pi^2}{6}$ concluimos

$$\sum_{n\leq x}\phi(n) = \frac{x^2}{2\zeta(2)} + O(x\log(x)).$$

Para demostrar 1.8 hacemos un razonamiento análogo. Consideremos la relación

$$\frac{\phi(n)}{n} = \sum_{d|n}\frac{\mu(d)}{d}$$

y obtenemos

$$\sum_{n\leq x}\frac{\phi(n)}{n} = \sum_{n\leq x}\sum_{d|n}\frac{\mu(d)}{d} = \sum_{\substack{q,d\\ qd\leq x}}\frac{\mu(d)}{d} = \sum_{d\leq x}\frac{\mu(d)}{d}\sum_{q\leq\frac{x}{d}}1.$$

Usando la relación 1.4 con $\alpha = 0$ tenemos

$$\begin{aligned}\sum_{n\leq x}\frac{\phi(n)}{n} &= \sum_{d\leq x}\frac{\mu(d)}{d}\left(\left(\frac{x}{d}\right) + O(1)\right)\\ &= x\sum_{d\leq x}\frac{\mu(d)}{d^2} + O\left(\sum_{d\leq x}\frac{1}{d}\right).\end{aligned}$$

por las estimativas 1.3 y 1.6 obtenemos

$$\sum_{n\leq x}\frac{\phi(n)}{n} = x\left(\frac{6}{\pi^2} + O\left(\frac{1}{x}\right)\right) + O(\log x) = \frac{6}{\pi^2}x + O(\log x).$$

Haciendo $\zeta(2) = \frac{\pi^2}{6}$ concluimos

$$\sum_{n\leq x}\frac{\phi(n)}{n} = \frac{x}{\zeta(2)} + O(\log(x)).$$

$\blacksquare$

Para obtener la cota superior para el caso especial $f(n)$ nos ayudamos del teorema 3.1 de [4] y de la media aritmética-geométrica que enunciamos a continuación.

Teorema 1.13. *La función* $g(n) = \sum_{i=1}^{n}(i, n)$ *esta acotada por las expresiones:*

$$max(2 - \frac{1}{n}, \left(\frac{3}{2}\right)^{w(n)}) \leq \frac{g(n)}{n} \leq 27 \left(\frac{\log n}{w(n)}\right)^{w(n)}$$

donde n *es un número entero positivo y* $w(n)$ *es el número de primos distintos que dividen a* n*.*

Nos limitaremos a obtener la cota superior, la cual necesitaremos para la demostración de la cota superior de $f(n)$. Sin embargo en [4] se da una demostración para la cota inferior de este teorema.

Demostración. Para obtener la cota superior necesitaremos del teorema 2.2 de [4], el cual nos da una evaluación para la función $g(n) = \sum_{i=1}^{n}(i, n)$ cuando $n = p^{\alpha}$, $\alpha \geq 1$. Está es $g(p^{\alpha}) = (\alpha + 1)p^{\alpha} - \alpha p^{\alpha-1}$.
Por la ecuación anterior tenemos que

$$\frac{g(p^{\alpha})}{p^{\alpha}} = \alpha(1 - \frac{1}{p}) + 1 \leq w\alpha \log p,$$

donde $w = 3$ si $p = 2, 3, 5$ o $w = 1$ si $p \geq 7$. Luego, si $p_i \geq 7$ para todo i y $n = \prod_{i=1}^{m} p_i^{\alpha_i}$, tenemos

$$\frac{g(n)}{n} \leq \prod_{i=1}^{m} \alpha_i \log p_i = \prod_{i=1}^{m} \log(p_i^{\alpha_i}).$$

También podemos concluir que $\log n = \sum_{i=1}^{m} \alpha_i \log p_i$.
Si f es una función $f(x) = \prod_{i=1}^{m} x_i$ con $x_i \geq 1$ y $\sum x_i = \alpha$, para algún $\alpha \geq 0$,

entonces (usando multiplicadores de Lagrange) el máximo valor de f es $\left(\frac{\alpha}{m}\right)^m$ y se produce cuando cada $x_i = \frac{\alpha}{m}$. Por consiguiente

$$\frac{g(n)}{n} \leq \left(\frac{\log n}{m}\right)^m = \left(\frac{\log n}{w(n)}\right)^{w(n)}.$$

En general, usando $\alpha_1 = 1$, si $2 \nmid n$, etc,

$$\begin{aligned}
\frac{g(n)}{n} &\leq 27(\alpha_1 \log p_1)(\alpha_2 \log p_2)(\alpha_3 \log p_3) \prod_{p_i \geq 7} \alpha_i \log p_i \\
&= 27 \prod_{i=1}^{m} \alpha_i \log p_i \\
&\leq 27 \left(\frac{\log n}{w(n)}\right)^{w(n)}.
\end{aligned}$$

■

Si $x_1, x_2, ..., x_n$ son números reales no negativos entonces

$$\frac{x_1 + x_2 + ... + x_n}{n} \geq \sqrt[n]{x_1 x_2 ... x_n}$$

y la igualdad se da solamente si $x_1 = x_2 = ... = x_n$.

Una demostración es la siguiente: sea

$$A = \frac{x_1 + x_2 + ... + x_n}{n}$$

la media aritmética de dichos números. Para cada k incorporemos $a_k := \frac{x_k}{A} - 1$ en la desigualdad $1 + a \leq e^a \quad (a \geq 0)$. Puesto que $\frac{x_k}{A} = 1 + a_k \leq e^{a_k}$, deducimos multiplicando cada uno de estos términos que

$$\frac{x_1 x_2 ... x_n}{A^n} \leq e^{a_1} \cdot e^{a_2} \cdot ... \cdot e^{a_n} = e^{a_1 + a_2 + ... + a_n} = 1$$

Donde concluimos

$$x_1 x_2 ... x_n \leq A^n.$$

Así mismo la igualdad se cumple si y solo si $x_1 = x_2 = ... = x_n$.

Antes de dar a conocer el teorema que nos da el número de soluciones de $x^{n-1} \equiv 1\,(mod\, n)$, considerado como una de las aplicaciones de $g(n)$, recordemos los siguientes teoremas.

Teorema 1.14. *Si p es primo y $(a,p) = 1$, entonces la congruencia $x^n \equiv a\,(mod\, p)$ tiene soluciones si y solo si*

$$a^{(p-1)/(n,p-1)} \equiv 1(mod\, p).$$

Si tiene una solución tiene $(n, p-1)$ soluciones.

Demostración. Sea g una raíz primitiva $(mod\, p)$, y elijamos i tal que $g^i \equiv a\,(mod\, p)$. Si hay una x tal que $x^n \equiv a\,(mod\, p)$ entonces $(x,p) = 1$, de manera que $x \equiv g^u\,(mod\, p)$ para alguna u. Así la congruencia propuesta es $g^{nu} \equiv g^i\,(mod\, p)$, la cual es equivalente a $nu \equiv i\,(mod\, p-1)$. Sea $k = (n, p-1)$. Por el teorema 2.17 en [11] , esta tiene k soluciones si $k|i$, y no tiene solución si $k \nmid i$. Si $k|i$, entonces $\frac{i(p-1)}{k} \equiv 0\,(mod\, p-1)$, de manera que $a^{(p-1)/k} \equiv g^{i(p-1)/k} = (g^{p-1})^{i/k} \equiv 1\,(mod\, p)$. Por otro lado, si $k \nmid i$ entonces $i(p-1)/k \not\equiv 0\,(mod\, p-1)$ y por lo tanto $a^{(p-1)/k} \equiv g^{i(p-1)/k} \not\equiv 1\,(mod\, p)$. ■

Teorema 1.15. *Supongamos que $\alpha \geq 2$ y que r es una solución de la congruencia*

$$f(x) \equiv 0\,(mod\, p^{\alpha-1}) \tag{1.9}$$

que pertenece al intervalo $0 \leq r < p^{\alpha-1}$.

a) Suponemos que $f'(r) \not\equiv 0\,(mod\, p)$. Entonces r puede subirse de forma única de $p^{\alpha-1}$ a p^α. Esto es, existe un único a en el intervalo $0 \leq a < p^\alpha$ que genera a r y que satisface la congruencia

$$f(x) \equiv 0\,(mod\, p^\alpha). \tag{1.10}$$

b) Suponemos $f'(r) \equiv 0 \,(mod\, p)$. Entonces tenemos dos posibilidades:

- I) *Si $f(r) \equiv 0 \,(mod\, p^{\alpha})$, r puede subirse de $p^{\alpha-1}$ a p^{α} de p formas distintas.*
- II) *Si $f(r) \not\equiv 0 \,(mod\, p^{\alpha})$, r no puede subirse de $p^{\alpha-1}$ a p^{α}.*

Demostración. Si n es el grado de f tenemos la identidad (fórmula de Taylor)

$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + ... + \frac{f^{(n)}(x)}{n!}h^n \tag{1.11}$$

para cada x y h. Observemos que cada polinomio $\frac{f^{(k)}(x)}{k!}$ tiene coeficientes enteros. Ahora hacemos $x = r$ en (1.11), en donde r es una solución de (1.9) perteneciente al intervalo $0 \leq r < p^{\alpha-1}$, y sea $h = qp^{\alpha-1}$ en donde q es un entero que a continuación especificaremos. Dado que $\alpha \geq 2$, los términos de (1.11) que contienen h^2 y potencias superiores de h son múltiplos enteros de p^{α}. Por consiguiente (1.11) nos da la congruencia

$$f(r + qp^{\alpha-1}) \equiv f(r) + f'(r)qp^{\alpha-1}(mod\, p^{\alpha}).$$

Puesto que r satisface (1.9) podemos escribir $f(r) = kp^{\alpha-1}$ para algún entero k, y la ultima congruencia nos conduce a

$$f(r + qp^{\alpha-1}) \equiv \{qf'(r) + k\}p^{\alpha-1}(mod\, p^{\alpha}).$$

Sea ahora

$$a = r + qp^{\alpha-1}. \tag{1.12}$$

Entonces a satisface la congruencia (1.10) si y solo si q satisface la congruencia lineal

$$qf'(r) + k \equiv 0(mod\, p). \tag{1.13}$$

Si $f'(r) \not\equiv 0 \,(mod\, p)$ esta congruencia tiene una solución única $q \,mod\, p$, y si elegimos q en el intervalo $0 \leq q < p$ entonces el número a dado por (1.12) satisfará (1.10) y pertenecerá al intervalo $0 \leq a < p^{\alpha}$.

Por otro lado, si $f'(r) \not\equiv 0\,(mod\, p)$ entonces (1.13) tiene una solución q si y solo si, $p|k$, esto es, si y solo si $f(r) \equiv 0\,(mod\, p^{\alpha})$. Si $p \nmid k$ no existe ninguna elección de q tal que a satisfaga (1.10), pero, si $p \mid k$, entonces los p valores $q = 0, 1, ..., p-1$ dan p soluciones a de (1.10) que generan r y pertenecen al intervalo $0 \leq a < p^{\alpha}$.

■

Teorema 1.16. *Sea* $n = \prod p_i^{\alpha_i}$ *un entero positivo. Entonces el número de soluciones distintas módulo* n *de*

$$x^{n-1} \equiv 1\,(mod\, n)$$

está dado por la fórmula

$$\prod_{p|n}(n-1, p-1).$$

Demostración. Sea

$$f(x) = x^{n-1} - 1 \equiv 0\,(mod\, n). \tag{1.14}$$

Consideremos las congruencias

$$f(x) \equiv 0\,(mod\, p_i^{\alpha_i}), \tag{1.15}$$

$$f(x) \equiv 0\,(mod\, p). \tag{1.16}$$

Por el teorema 1.14 la congruencia (1.16) tiene $d = (n-1, p-1)$ soluciones distintas modulo p. Notemos que $d \geq 2$ si n es impar, en este caso tanto $n-1$ como $p-1$ son pares.

Por el teorema 1.15, cada solución r de (1.16) corresponde a una solución de (1.15) (pues $f'(r) \not\equiv 0\,(mod\, n)$) y viceversa. Así (1.15) tiene d soluciones distintas modulo $p_i^{\alpha_i}$. Finalmente usando el teorema chino de los residuos, (1.14) tiene $\prod d$ soluciones distintas modulo n, incluyendo las soluciones triviales $x \equiv \pm 1\,(mod\, n)$.

■

Definición 1.17. ***Números seudoprimos***

Sea n un número entero compuesto impar, y sea b un entero primo relativo con n. Decimos que n es un seudoprimo de base b si

$$b^{n-1} \equiv 1 \, (mod \, n). \tag{1.17}$$

Al conjunto de bases de seudoprimalidad de n la denotaremos por

$$Sp(n) = \{b \in \mathbb{Z} | b^{n-1} \equiv 1 \, (mod \, n)\}$$

y diremos que n es $Sp(b)$.

Es claro que el teorema 1.16 está relacionado con las bases de seudoprimalidad de n. La razón de llamar seudoprimo a un número entero positivo, se encuentra en el pequeño teorema de Fermat $x^{p-1} \equiv 1 \, (mod \, p)$, donde p es un número primo, comparado con (1.17).

Capítulo 2

Evaluaciones, identidades y propiedades de la función $g(n;h)$

En este capítulo estudiaremos algunas evaluaciones, identidades y propiedades de la función definida por:

$$g(n;h) := \prod_{j=1}^{n} h((j,n)), \tag{2.1}$$

donde $(j,n) := mcd(j,n)$ es el máximo común divisor de j y n, y $h(x)$ es una función aritmética. Para el caso $e(x) := x$ denotamos $g(n) = g(n;e)$ y definimos:

$$g(n) := \prod_{j=1}^{n} (j,n). \tag{2.2}$$

Esto convierte a (2.1) en una generalización de (2.2).

Observemos que si en (2.1) $n = p$, p primo, tenemos:

$$\begin{aligned} g(p;h) &= \prod_{j=1}^{p} h((j,p)) \\ &= h((1,p)) \cdot h((2,p)) \cdot h((3,p)) \cdot ... \cdot h((p-1,p)) \cdot h((p,p)) \end{aligned}$$

$$= \underbrace{h(1) \cdot h(1) \cdot h(1) \cdot ... \cdot h((1))}_{p-1\, veces} \cdot h(p)$$

$$= h(1)^{p-1} h(p). \tag{2.3}$$

Ahora consideraremos (2.1) cuando $n = p^\alpha$.

Teorema 2.1. *Si p es primo y α es un entero positivo, entonces*

$$g(p^\alpha; h) = \frac{h(p^\alpha)}{h(p^{\alpha-1})} g(p^{\alpha-1}; h)^p.$$

Demostración.

$$\begin{aligned}
g(p^\alpha; h) &= \prod_{j=1}^{p^\alpha} h((j, p^\alpha)) \\
&= \prod_{j=1}^{p^{\alpha-1}} h((j, p^\alpha)) \prod_{j=p^{\alpha-1}+1}^{2p^{\alpha-1}} h((j, p^\alpha)) ... \prod_{j=(p-1)p^{\alpha-1}+1}^{p^\alpha} h((j, p^\alpha)) \\
&= \frac{h(p^\alpha)}{h(p^{\alpha-1})} \prod_{j=1}^{p^{\alpha-1}} h((j, p^{\alpha-1})) \prod_{j=1}^{p^{\alpha-1}} h((j, p^{\alpha-1})) ... \prod_{j=1}^{p^{\alpha-1}} h((j, p^{\alpha-1})) \\
&= \frac{h(p^\alpha)}{h(p^{\alpha-1})} g(p^{\alpha-1}; h)^p.
\end{aligned}$$

■

El siguiente teorema nos da otra evaluación de la función (2.1) cuando $n = p^\alpha$, la cual depende solo de h.

Teorema 2.2. *Si p es primo y α es un entero positivo, entonces*

$$g(p^\alpha; h) = h(p^\alpha) \prod_{j=0}^{\alpha-1} h(p^j)^{(p-1)p^{\alpha-j-1}}. \tag{2.4}$$

Demostración. Por inducción sobre α:

I. Si $\alpha = 1$ tenemos $g(p; h) = h(p)h(1)^{p-1}$ obtenida en (2.3)

II. Consideremos este resultado verdadero para $\alpha = k$. Por lo tanto

$$\begin{aligned}
g(p^{k+1};h) &= \frac{h(p^{k+1})}{h(p^k)} g(p^k;h)^p \\
&= \frac{h(p^{k+1})}{h(p^k)} \left(h(p^k) \prod_{j=0}^{k-1} h(p^j)^{(p-1)p^{k-j-1}} \right)^p \\
&= h(p^{k+1}) h(p^k)^{p-1} \prod_{j=0}^{k-1} h(p^j)^{(p-1)p^{k-j}} \\
&= h(p^{k+1}) \prod_{j=0}^{k} h(p^j)^{(p-1)p^{k-j}} \\
&= h(p^{k+1}) \prod_{j=0}^{k} h(p^j)^{(p-1)p^{(k+1)-j-1}}
\end{aligned}$$

■

Consideremos los siguientes ejemplos.

Ejemplo 2.3. *Sea* $h(x) := \sqrt{\sqrt{x} + x}$, *entonces*

$$\begin{aligned}
g(17^2;h) &= \prod_{j=1}^{17^2} \sqrt{\sqrt{(j,17^2)} + (j,17^2)} \\
&= h(17^2) \prod_{j=0}^{2-1} h(17^j)^{(17-1)17^{1-j}} \\
&= \sqrt{\sqrt{17^2} + 17^2} \left(\sqrt{1+1}^{(17-1)17} \sqrt{\sqrt{17} + 17}^{17-1} \right) \\
&= 2^{136} \sqrt{306} (\sqrt{17} + 17)^8.
\end{aligned}$$

Ejemplo 2.4. *Sea* $h(x) := e^{\frac{2\pi i}{x}}$, *entonces*

$$g(23^2;h) = \prod_{j=1}^{23^2} e^{\frac{2\pi i}{(j,23^2)}}$$

$$
\begin{aligned}
&= h(23^2)\prod_{j=0}^{2-1} h(23^j)^{(23-1)23^{1-j}} \\
&= e^{\frac{2\pi i}{23^2}}(e^{2\pi i})^{22*23}(e^{\frac{2\pi i}{23}})^{22} \\
&= e^{\frac{536362}{23^2}\pi i}.
\end{aligned}
$$

En la teoría de las funciones aritméticas es común preguntarnos si la función aritmetica considerada es o no multiplicativa. En nuestro caso, las funciones $g(n)$ y $g(n;h)$ no cumplen con la multiplicidad, pero satisfacen, sin embargo, la siguiente relación.

Teorema 2.5. *Si $h(x)$ es multiplicativa y m y n son enteros con $(m,n)=1$, entonces*

$$
g(mn;h) = [g(m;h)]^n[g(n;h)]^m. \tag{2.5}
$$

Demostración. Como $(m,n)=1$ y j es un entero positivo, tenemos, usando la multiplicidad de h que

$$
h((j,mn)) = h((j,n)(j,m)) = h((j,n))h((j,m)).
$$

Entonces

$$
\begin{aligned}
g(mn;h) &= \prod_{j=1}^{mn} h((j,mn)) \\
&= \left[\prod_{j=1}^{mn} h((j,m))\right]\left[\prod_{j=1}^{mn} h((j,n))\right] \\
&= \left[\prod_{j=1}^{m} h((j,m))\right]^n\left[\prod_{j=1}^{n} h((j,n))\right]^m \\
&= [g(m;h)]^n[g(n;h)]^m.
\end{aligned}
$$

■

Si en la relación anterior elevamos a la $\frac{1}{mn}$ a los dos lados tenemos

$$\begin{aligned} g(mn;h)^{\frac{1}{mn}} &= ([g(m;h)]^n[g(n;h)]^m)^{\frac{1}{mn}} \\ &= [g(m;h)]^{\frac{1}{m}}[g(n;h)]^{\frac{1}{n}}. \end{aligned}$$

Esto nos da la posibilidad de definir la función $f(n;h) := g(n;h)^{\frac{1}{n}}$ que es entonces multiplicativa, cuando $h(x)$ es multiplicativa. Además podemos visualizar algunas propiedades de $f(n;h)$ análogas a $g(n;h)$ en el siguiente teorema.

Teorema 2.6. *Si $h(x)$ es multiplicativa, entonces la función $f(n;h) = g(n;h)^{\frac{1}{n}}$ satisface las siguientes propiedades:*

I. *Si p es primo y α es un entero positivo, entonces*

$$f(p^\alpha;h) = h(p^\alpha)^{p^{-\alpha}} \prod_{j=0}^{\alpha-1} h(p^j)^{(p-1)p^{-j-1}}. \tag{2.6}$$

II. *Si m y n son enteros con $(m,n) = 1$, entonces*

$$f(mn;h) = f(m;h)f(n;h). \tag{2.7}$$

Demostración. I. Por definición tenemos que

$$f(p^\alpha;h) = g(p^\alpha;h)^{p^{-\alpha}};$$

entonces por (2.4) tenemos

$$\begin{aligned} f(p^\alpha;h) &= \left(h(p^\alpha) \prod_{j=0}^{\alpha-1} h(p^j)^{(p-1)p^{\alpha-j-1}} \right)^{p^{-\alpha}} \\ &= h(p^\alpha)^{p^{-\alpha}} \prod_{j=0}^{\alpha-1} h(p^j)^{(p-1)p^{-j-1}}. \end{aligned}$$

II. Análogamente, tenemos por definición

$$f(mn;h) = g(mn;h)^{\frac{1}{mn}}$$

entonces por (2.5) deducimos que

$$\begin{aligned} f(mn;h) &= ([g(m;h)^n][g(n;h)^m])^{\frac{1}{mn}} \\ &= [g(m;h)^n]^{\frac{1}{mn}}[g(n;h)^m]^{\frac{1}{mn}} \\ &= f(m;h)f(n;h). \end{aligned}$$

■

Ahora, vamos a obtener evaluaciones generales para $g(n;h)$ y $f(n;h)$ cuando $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ y $h(x)$ multiplicativa.
Si usamos (2.6) con $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ tenemos

$$f\left(\prod_{i=1}^{k} p_i^{\alpha_i};h\right) = h\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)^{p_i^{-\alpha_i}} \prod_{j=0}^{\alpha_i-1} h\left(\left(\prod_{i=1}^{k} p_i\right)^j\right)^{(p_i-1)p_i^{-j-1}}$$

y como $h(x)$ es multiplicativa obtenemos

$$f\left(\prod_{i=1}^{k} p_i^{\alpha_i};h\right) = \prod_{i=1}^{k}\left[h(p_i^{\alpha_i})^{p_i^{-\alpha_i}} \prod_{j=0}^{\alpha_i-1} h(p_i^j)^{(p_i-1)p_i^{-j-1}}\right].$$

Ademas, como $f(n;h) := g(n;h)^{\frac{1}{n}}$, nos resulta que

$$g\left(\prod_{i=1}^{k} p_i^{\alpha_i};h\right) = \left(\prod_{i=1}^{k}\left[h(p_i^{\alpha_i})^{p_i^{-\alpha_i}} \prod_{j=0}^{\alpha_i-1} h(p_i^j)^{(p_i-1)p_i^{-j-1}}\right]\right)^n.$$

Estas observaciones las podemos resumir en el siguiente corolario

Corolario 2.7. *Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ es la factorización prima de n y $h(x)$ es multiplicativa, entonces*

$$f(n;h) = \prod_{i=1}^{k}\left[h(p_i^{\alpha_i})^{p_i^{-\alpha_i}} \prod_{j=0}^{\alpha_i-1} h(p_i^j)^{(p_i-1)p_i^{-j-1}}\right] \tag{2.8}$$

y

$$g(n;h) = \left(\prod_{i=1}^{k}\left[h(p_i^{\alpha_i})^{p_i^{-\alpha_i}}\prod_{j=0}^{\alpha_i-1}h(p_i^j)^{(p_i-1)p_i^{-j-1}}\right]\right)^n. \tag{2.9}$$

Para las funciones $g(n)$ y $f(n)$ tenemos los siguientes corolarios:

Corolario 2.8. *Las funciones $g(n)$ y $f(n)$ donde $f(n) = g(n)^{\frac{1}{n}}$, satisfacen las siguientes propiedades:*

I *Si p es primo y a es un entero positivo, entonces*

$$g(p^\alpha) = p^{\frac{p^\alpha-1}{p-1}} \quad y \quad f(p^\alpha) = p^{\frac{1-p^{-\alpha}}{p-1}}$$

II *Si m y n son enteros positivos con $(m,n) = 1$, entonces*

$$f(mn) = f(m)f(n).$$

Demostración. I. Haciendo $h(x) = e(x) := x$ en (2.6) tenemos

$$\begin{aligned} g(p^\alpha) = g(p^\alpha; e) &= p^\alpha \prod_{j=0}^{\alpha-1}(p^j)^{(p-1)p^{\alpha-j-1}} \\ &= p^\alpha p^{(p-1)p^{\alpha-1}\Sigma_{j=0}^{\alpha-1} j(\frac{1}{p})^j} \\ &= p^\alpha p^{(p-1)p^{\alpha-1}\frac{(\alpha-1/p^\alpha)-\alpha/p^{\alpha-1}+1}{p(1-1/p)^2}} \\ &= p^\alpha p^{(p-1)\frac{\alpha-1-\alpha p+p^\alpha}{(p-1)^2}} \\ &= p^{\alpha+\frac{\alpha-1-\alpha p+p^\alpha}{p-1}} = p^{\frac{p^\alpha-1}{p-1}}. \end{aligned}$$

Como $f(p^\alpha) = g(p^\alpha)^{\frac{1}{p^\alpha}}$ tenemos $f(p^\alpha) = \left(p^{\frac{p^\alpha-1}{p-1}}\right)^{\frac{1}{p^\alpha}} = p^{\frac{1-p^{-\alpha}}{p-1}}$

II. Por (2.7) tenemos que $f(mn) = f(m)f(n)$ con $(m,n) = 1$ ■

El siguiente corolario muestra las evaluaciones para $f(n)$ y $g(n)$ que obtenemos haciendo $h(x) = e(x) := x$ en (2.8) y (2.9) respectivamente.

Corolario 2.9. *Si* $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ *es la factorización prima de* n*, entonces*

$$f(n) = \prod_{i=1}^{k} p_i^{\frac{1-p_i^{-\alpha_i}}{p_i-1}} \quad y \quad g(n) = \left[\prod_{i=1}^{k} p_i^{\frac{1-p_i^{-\alpha_i}}{p_i-1}}\right]^n$$

.

Por último, encontraremos algunas identidades que relacionan la función $g(n;h)$ con la función $\phi(n)$, importantes en la deducción de la serie de Dirichlet. Recordemos que para cada entero positivo n, definimos $\phi(n)$ como el número de enteros positivos menores o iguales que n y primos relativos con n. También recordemos que si $e|n$, el número de enteros en el conjunto $S = \{1, 2, 3, ..., n\}$ que tienen con n como máximo común divisor a e es $\phi\left(\frac{n}{e}\right)$. Es decir, el número de enteros j con $1 \leq j \leq n$ tal que $(j, n) = e$, esta dado por $\phi\left(\frac{n}{e}\right)$

Usando estas observaciones evaluaremos la función $g(n;h)$ en términos de $\phi(d)$, donde d representa los divisores de n.

$$g(n;h) = \prod_{j=1}^{n} h((j,n)) = \prod_{e|n} h(e)^{\phi(\frac{n}{e})} = \prod_{d|n} h\left(\frac{n}{d}\right)^{\phi(d)} \tag{2.10}$$

Si consideramos la ecuación

$$g(n;h) = \prod_{e|n} h(e)^{\phi(\frac{n}{e})} = h(e_1)^{\phi\left(\frac{n}{e_1}\right)} \cdot h(e_2)^{\phi\left(\frac{n}{e_2}\right)} \cdot ... \cdot h(e_n)^{\phi\left(\frac{n}{e_n}\right)}$$

donde e_1, e_2,..., e_n son los divisores de n, y aplicamos logaritmos a ambos lados tenemos:

$$\begin{aligned}
log[g(n;h)] = log\left[\prod_{e|n} h(e)^{\phi(\frac{n}{e})}\right] &= log\left[h(e_1)^{\phi\left(\frac{n}{e_1}\right)} \cdot h(e_2)^{\phi\left(\frac{n}{e_2}\right)} \cdot ... \cdot h(e_n)^{\phi\left(\frac{n}{e_n}\right)}\right] \\
&= log[h(e_1)]^{\phi\left(\frac{n}{e_1}\right)} + log[h(e_2)]^{\phi\left(\frac{n}{e_2}\right)} + ... + log[h(e_n)]^{\phi\left(\frac{n}{e_n}\right)} \\
&= \phi\left(\frac{n}{e_1}\right) log[h(e_1)] + \phi\left(\frac{n}{e_2}\right) log[h(e_2)] + ... + \phi\left(\frac{n}{e_n}\right) log[h(e_n)] \\
&= \sum_{e|n} \phi\left(\frac{n}{e}\right) log[h(e)].
\end{aligned}$$

Análogamente, llegamos a la identidad

$$log[g(n;h)] = \sum_{d|n} \phi(d) log \left[h\left(\frac{n}{d}\right)\right]$$

que resumiremos en el siguiente teorema.

Teorema 2.10. *Si n es un entero positivo, entonces*

$$log[g(n;h)] = \sum_{e|n} \phi\left(\frac{n}{e}\right) log[h(e)] = \sum_{d|n} \phi(d) log \left[h\left(\frac{n}{d}\right)\right]. \tag{2.11}$$

Haciendo $h(x) := x$ concluimos:

Teorema 2.11. *Si n es un entero positivo, entonces $g(n) = n^n \prod_{d|n} \frac{1}{d^{\phi(d)}}$.*

Demostración. Usando la relación dada en (2.10) tenemos que

$$g(n) = \prod_{d|n} \left(\frac{n}{d}\right)^{\phi(d)} = n^{\sum_{d|n} \phi(d)} \prod_{d|n} \frac{1}{d^{\phi(d)}}.$$

y para cada entero n, tenemos $\sum_{d|n} \phi(d) = n$, entonces

$$g(n) = n^n \prod_{d|n} \frac{1}{d^{\phi(d)}}$$

$\blacksquare$

Capítulo 3

Series de Dirichlet y comportamientos asintóticos

En este capítulo estudiaremos las series de Dirichlet para $\log[g(n;h)]$ las cuales evaluaremos en términos de la función zeta de Riemann y la serie $\sum_{n=1}^{\infty}\frac{\log[h(n)]}{n^s}$. Además trataremos algunos comportamientos asintóticos para $g(n;h)$ y para el caso especial $g(n)$.

Empecemos por definir la serie de Dirichlet para $\log[g(n;h)]$ de la siguiente forma

$$G(s;h)=\sum_{n=1}^{\infty}\frac{\log[g(n;h)]}{n^s}=\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}\log[h((j,n))]}{n^s} \tag{3.1}$$

para $s\in A_h$, donde $A_h\subseteq\mathbb{C}$ es el conjunto de valores que dependen de h para los cuales la serie converge.

Ahora vamos a evaluar (3.1) en términos de la función zeta de Riemann y la serie $\sum_{n=1}^{\infty}\frac{\log[h(n)]}{n^s}$. Para esto, analicemos la convergencia de $\sum_{n=1}^{\infty}\frac{\log[h(n)]}{n^s}$ y definamos para una función $h(x)$, el conjunto S_h y la constante c_h de la siguiente manera

$$S_h=\{\alpha\in\mathbb{R}|\log[h(n)]=O(n^{\alpha})\text{ cuando }n\to\infty\}\text{ y }c_h=\text{máx}\{2,1+\text{ínf }S_h\}.$$

Nos limitaremos a las funciones $h(x)$ tal que el conjunto S_h sea no vacío. La definición de c_h es necesaria para garantizar la convergencia de las series $\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}$ y $\sum_{n=1}^{\infty} \frac{\log[h(n)]}{n^s}$. Estas expresiones están relacionadas con la convergencia de la serie de Dirichlet para (3.1) que resumiremos en el siguiente teorema.

Teorema 3.1. *La serie de Dirichlet para $G(s;h)$ converge para $Re(s) > c_h$. Además, en este dominio*

$$G(s;h) = \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{n=1}^{\infty} \frac{\log[h(n)]}{n^s}\right),$$

donde $\zeta(s)$ es la función zeta de Riemann.

Demostración. Usando el teorema 2.10 y la definición 1.6, tenemos

$$\log[g(n;h)] = \phi(d)\log[h\left(\frac{n}{d}\right)] = (\phi * (\log \circ h))(n).$$

Entonces, por el teorema 1.5 tenemos

$$\begin{aligned} G(s;h) &= \sum_{n=1}^{\infty} \frac{\log[g(n;h)]}{n^s} \\ &= \left(\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\log[h(n)]}{n^s}\right); \end{aligned}$$

por lo tanto, por (1.7), tenemos

$$G(s;h) = \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{n=1}^{\infty} \frac{\log[h(n)]}{n^s}\right) \quad para \quad Re(s) > c_h$$

■

Definamos ahora la función $h^{(\alpha)}(x) = x^\alpha$ y consideremos los casos especiales $G(s;h^{(\alpha)})$ y $G(s;exp \circ h)$.

Por (3.1) tenemos

$$G(s;h^{(\alpha)}) = \sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} \log[(j,n)^\alpha]}{n^s}, \tag{3.2}$$

que por el teorema anterior, queda como

$$\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}\log[(j,n)^{\alpha}]}{n^s}=\left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\alpha\sum_{n=1}^{\infty}\frac{\log n}{n^s}\right),$$

de donde concluimos, por (1.2), que

$$G(s;h^{(\alpha)})=\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}\log[(j,n)^{\alpha}]}{n^s}=-\frac{\alpha\zeta(s-1)\zeta'(s)}{\zeta(s)}\quad para\quad s>2. \tag{3.3}$$

Análogamente, por (3.1) tenemos

$$G(s;exp\circ h)=\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}h((j,n))}{n^s}, \tag{3.4}$$

y tenemos

$$\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}h((j,n))}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}\left(\sum_{n=1}^{\infty}\frac{h(n)}{n^s}\right)\quad para\quad s>c_{exp(h(x))}. \tag{3.5}$$

Usando (3.3) y (3.5) obtenemos algunas identidades que resumiremos en el siguiente corolario.

Corolario 3.2. *Para todo α, $\beta\in\mathbb{R}$ tenemos las siguientes relaciones:*

I). $\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}(j,n)^{\alpha}}{n^s}=\frac{\zeta(s-1)\zeta(s-\alpha)}{\zeta(s)}\quad para\quad Re(s)>max\{2,\alpha+1\}.$

II). $\frac{\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}h((j,n))}{n^s}}{\sum_{n=1}^{\infty}\frac{h(n)}{n^s}}=\frac{\zeta(s-1)}{\zeta(s)}\quad para\quad Re(s)>c_{exp(h(x))}.$

III). $\frac{\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}h_1((j,n))}{n^s}}{\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}h_2((j,n))}{n^s}}=\frac{\sum_{n=1}^{\infty}\frac{h_1(n)}{n^s}}{\sum_{n=1}^{\infty}\frac{h_2(n)}{n^s}}\quad para\quad Re(s)>max\{c_{exp(h_1(x))},c_{exp(h_2(x))}\}.$

IV). $\frac{\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}(j,n)^{\alpha}}{n^s}}{\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}(j,n)^{\beta}}{n^s}}=\frac{\zeta(s-\alpha)}{\zeta(s-\beta)}\quad para\quad Re(s)>max\{2,\alpha+1,\beta+1\}.$

V). $\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}\phi((j,n))}{n^s}=\frac{\zeta^2(s-1)}{\zeta^2(s)}\quad para\quad Re(s)>2.$

Demostración. I). Sustituyendo $h^{\alpha}(x)=x^{\alpha}$ en (3.5) tenemos

$$\sum_{n=1}^{\infty}\frac{\sum_{j=1}^{n}(j,n)^{\alpha}}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}\left(\sum_{n=1}^{\infty}\frac{n^{\alpha}}{n^s}\right)=\frac{\zeta(s-1)\zeta(s-\alpha)}{\zeta(s)}$$

para $Re(s)>max\{2,\alpha+1\}$.

II). Es inmediato de (3.5).

III). Consideremos dos ecuaciones de la forma (3.5) para $h_1(x)$ y $h_2(x)$ si hacemos el cociente entre las dos ecuaciones obtenemos el resultado deseado.

IV). Si hacemos $h_1(x) = x^\alpha$ y $h_2(x) = x^\beta$ en III) tenemos

$$\frac{\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} (j,n)^\alpha}{n^s}}{\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} h_2(j,n)^\beta}{n^s}} = \frac{\sum_{n=1}^{\infty} \frac{n^\alpha}{n^s}}{\sum_{n=1}^{\infty} \frac{n^\beta}{n^s}} = \frac{\zeta(s-\alpha)}{\zeta(s-\beta)}$$

para $\quad Re(s) > max\{2, \alpha+1, \beta+1\}$.

V). Haciendo $h_1(x) = \phi(x)$ en (3.5) y usando (1.7), tenemos

$$\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} \phi(j,n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \left(\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} \right) = \frac{\zeta^2(s-1)}{\zeta^2(s)} \quad para \quad s > 2.$$

■

Estas identidades permiten visualizar la convergencia de estas series en términos de la función zeta. Por ejemplo, en la identidad II), si eligiéramos una función $h(x)$ de tal manera que $\frac{\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} h((j,n))}{n^s}}{\sum_{n=1}^{\infty} \frac{h(n)}{n^s}}$ fuera evaluada en forma cerrada, entonces dicha evaluación estaría dada por $\frac{\zeta(s-1)}{\zeta(s)}$. Es decir, tendríamos una forma inductiva de evaluar la función $\zeta(s)$ cuando s toma valores enteros positivos. Tal forma podría dar valores para $\zeta(3)$, $\zeta(5)$, etc. Sin embargo, sabemos que $\zeta(3)$ es irracional [13], [14], pero no sabemos aún si $\zeta(2k+1)$ es irracional para $k > 1$ (k es número entero positivo).

Como tenemos evaluaciones para $\zeta(2k)$ cuando k es un entero positivo, podemos dar evaluaciones para expresiones de la forma de la identidad IV). Por ejemplo, con $s = 8$, $\alpha = 2$ y $\beta = 4$ tenemos

$$\frac{\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} (j,n)^2}{n^8}}{\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} (j,n)^4}{n^8}} = \frac{\zeta(6)}{\zeta(4)} = \frac{2\pi^2}{21}.$$

Considerando $s = 8$, $\alpha = 4$ y $\beta = 6$ tenemos

$$\frac{\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n}(j,n)^4}{n^8}}{\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n}(j,n)^6}{n^8}} = \frac{\zeta(4)}{\zeta(2)} = \frac{\pi^2}{15}.$$

También podemos usar los resultados del teorema 3.1 y del corolario 3.2 para dar identidades entre series infinitas en términos de la función zeta de Riemann. Entre estas tenemos:

Teorema 3.3. *Si* $h(x)$ *es una función tal que* $\log(h(x))$ *se puede representar como la serie infinita* $\log[h(x)] = \sum_{k=1}^{\infty} a_k \left(\frac{1}{x}\right)^k$ *que converge uniformemente para* $x \geq 1$ *y para* $Re(s) > c_h$*, entonces tenemos*

$$\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} \log[h((j,n))]}{n^s} = \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{k=1}^{\infty} a_k \zeta(s+k)\right).$$

Demostración. Usando el desarrollo de la serie infinita, tenemos

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} \log[h((j,n))]}{n^s} &= \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{n=1}^{\infty} \frac{\log[h(n)]}{n^s}\right) \\
&= \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{n=1}^{\infty} \frac{\sum_{k=1}^{\infty} a_k \left(\frac{1}{n}\right)^k}{n^s}\right) \\
&= \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{k=1}^{\infty} a_k \sum_{n=1}^{\infty} \frac{1}{n^{s+k}}\right) \\
&= \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{k=1}^{\infty} a_k \zeta(s+k)\right).
\end{aligned}$$

■

Corolario 3.4. *Si Re(s)>2, entonces*

$$-\sum_{n=1}^{\infty} \frac{\sum_{j=1}^{n} \log\left[1 - \frac{1}{2(j,n)}\right]}{n^s} = \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{k=1}^{\infty} \frac{\zeta(s+k)}{2^k k}\right).$$

Demostración. Haciendo $h(x) = \frac{1}{1-\frac{1}{2x}}$ en el teorema 3.3, donde

$$\log(h(x)) = \log\left(\frac{1}{1-\frac{1}{2x}}\right) = -\log\left(1 - \frac{1}{2x}\right)$$

cuyo desarrollo de Taylor es

$$-\log\left(1-\frac{1}{2x}\right)=\sum_{k=1}^{\infty}\frac{1}{k}\left(\frac{1}{2x}\right)^k=\sum_{k=1}^{\infty}\frac{1}{2^k k}\left(\frac{1}{x}\right)^k$$

para $x>\frac{1}{2}$ y considerando $a_k=\frac{1}{2^k k}$ tenemos el resultado deseado. ■

Ahora estudiaremos algunos comportamientos asintóticos para la suma $\sum_{n\leq x}\log[g(n;h)]$, donde consideraremos el caso $h(n)=O(n^{\alpha})$ para n suficientemente grande y α un número real fijo no negativo. Para esto necesitaremos del siguiente lema.

Lema 3.5. *Si x y y son números reales tales que $x\geq y>1$, entonces*

$$0\leq\log\left(\frac{x}{y}\right)\leq\frac{\log^2(x)}{4\log(y)}.$$

Demostración. Sea $x>1$ y consideremos la función $a_x(y)=\log(y)\log\left(\frac{x}{y}\right)$ con dominio $[1,x]$. Derivando $a_x(y)$ con respecto a y tenemos

$$a'_x(y)=\frac{\log(x)}{y}-2\frac{\log(y)}{y}=\frac{1}{y}\left[\log(x)-2\log(y)\right].$$

Así, $a_x(y)$ alcanza un máximo cuando $\log(x)-2\log(y)=0$, que es, $y=\sqrt{x}$, ya que $a'_x(y)>0$ para $1\leq y<\sqrt{x}$ y $a'_x(y)<0$ para $\sqrt{x}<y\leq x$. Entonces, para todo $y\in[1,x]$ tenemos

$$a_x(y)=\log(y)\log\left(\frac{x}{y}\right)\leq\log(\sqrt{x})\log\left(\frac{x}{\sqrt{x}}\right)=\frac{1}{4}\log^2(x).$$

Por lo tanto

$$\log\left(\frac{x}{y}\right)\leq\frac{\log^2(x)}{4\log(y)}\quad para\quad 1<y\leq x.$$

■

En el siguiente teorema mostraremos comportamientos asintóticos para funciones que cumplen $h(n)=O(n^{\alpha}),\alpha\geq 0$ cuando $n\to\infty$

Teorema 3.6. *Si $h(x)$ satisface la relación $h(n) = O(n^\alpha)$ para n suficientemente grande y α un número real fijo no negativo, entonces se tiene la siguiente fórmula asintótica:*

$$\sum_{n\leq x} \log[g(n;h)] = \frac{H_h}{2\zeta(2)}x^2 + O(x\log^3(x)) \quad \textit{para } x \textit{ suficientemente grande,}$$

donde $H_h = \sum_{k=1}^{\infty} \frac{\log[h(k)]}{k^2}$.

Demostración. Por el teorema 2.10 tenemos que

$$\begin{aligned}\sum_{n\leq x} \log[g(n;h)] &= \sum_{n\leq x}\sum_{d|n} \log(h(d))\phi(\frac{n}{d}) = \sum_{d\leq x}\log(h(d))\sum_{e\leq \frac{x}{d}}\phi(e)\\ &= \sum_{d\leq x}\log(h(d))\Phi_0\left(\frac{x}{d}\right).\end{aligned}$$

Usando la estimación 1.7 tenemos

$$\sum_{n\leq x} \log[g(n;h)] = \underbrace{\frac{x^2}{2\zeta(2)}\sum_{d\leq x}\frac{\log(h(d))}{d^2}}_{(1)} + \underbrace{O\left(x\sum_{d\leq x}\frac{\log(h(d))}{d}\log\left(\frac{x}{d}\right)\right)}_{(2)}.$$

Al simplificar el término (1) en la anterior fórmula, tenemos

$$\frac{x^2}{2\zeta(2)}\sum_{d\leq x}\frac{\log(h(d))}{d^2} = \frac{x^2}{2\zeta(2)}\left[H_h - \sum_{d>x}\frac{\log(h(d))}{d^2}\right].$$

Como $h(n) = O(n^\alpha)$ para n suficientemente grande y α un número real fijo no negativo, tenemos

$$\begin{aligned}\frac{x^2}{2\zeta(2)}\sum_{d\leq x}\frac{\log(h(d))}{d^2} &= \frac{x^2}{2\zeta(2)}\left[H_h - O\left(\sum_{d>x}\frac{\alpha\log(d)}{d^2}\right)\right]\\ &= \frac{x^2}{2\zeta(2)}\left[H_h - O\left(\int_0^\infty \frac{\log(x)}{x^2}dx\right)\right]\\ &= \frac{x^2}{2\zeta(2)}\left[H_h - O\left(\frac{\log(x)}{x}\right)\right] = \frac{x^2 H_h}{2\zeta(2)} + O(x\log(x)).\end{aligned}$$

Para el término (2) de la misma fórmula usamos el lema 3.5 para obtener

$$x \sum_{d \leq x} \frac{\log(h(d))}{d} \log\left(\frac{x}{d}\right) = O\left(x \sum_{d \leq x} \frac{\log(h(d))}{d} \frac{\log^2(x)}{4\log(d)}\right).$$

Como $h(n) = O(n^\alpha)$ para n suficientemente grande y α un número real fijo no negativo, tenemos

$$x \sum_{d \leq x} \frac{\log(h(d))}{d} \log\left(\frac{x}{d}\right) = O\left(x \log^2(x) \sum_{d \leq x} \frac{1}{d}\right),$$

luego, usando la estimativa (1.3) concluimos que

$$x \sum_{d \leq x} \frac{\log(h(d))}{d} \log\left(\frac{x}{d}\right) = O(x \log^3 x).$$

Por lo tanto,

$$\sum_{n \leq x} \log[g(n;h)] = \frac{x^2 H_h}{2\zeta(2)} + O(x\log(x)) + O(x \log^3 x) = \frac{x^2 H_h}{2\zeta(2)} + O(x \log^3(x)).$$

■

En el teorema anterior hemos obtenido

$$\sum_{n \leq x} \log[g(n;h)] = \frac{H_h}{2\zeta(2)} x^2 + O(x \log^3(x)) \quad \textit{para } x \textit{ suficientemente grande,}$$

lo que podemos escribir como

$$\log\left(\prod_{n \leq x} g(n;h)\right) = \frac{H_h}{2\zeta(2)} x^2 + O(x \log^3(x)) \quad \textit{para } x \textit{ suficientemente grande}$$

y, en consecuencia,

$$\prod_{n \leq x} g(n;h) = e^{\frac{H_h}{2\zeta(2)} x^2} \underbrace{e^{O(x \log^3(x))}}_{1} \quad \textit{para } x \textit{ suficientemente grande.}$$

El error $e^{O(x \log^3(x))}$ lo simplificamos de la siguiente forma: si $f(x) = O(x \log^3(x))$, por definición tenemos que existe $M > 0$ tal que

$$|f(x)| \leq M x \log^3(x)$$

y para x suficientemente grande se tiene

$$e^{|f(x)|} \leq e^{Mx\log^3(x)} = \left(e^{Mx\log(x)}\right)^{\log^2(x)} = x^{Mx\log^2(x)},$$

de donde concluimos que

$$\prod_{n\leq x} g(n;h) = e^{\frac{H_h}{2\zeta(2)}x^2} O(x^{x\log^2(x)}) \quad \textit{para } x \textit{ suficientemente grande.}$$

Este resultado lo resumimos en el siguiente corolario;

Corolario 3.7. *Si $h(x)$ satisface la relación $h(n) = O(n^\alpha)$ para n suficientemente grande y α un número real fijo no negativo, entonces se tiene la siguiente relación asintótica*

$$\prod_{n\leq x} g(n;h) = e^{\frac{H_h}{2\zeta(2)}x^2} O(x^{x\log(x)}) \quad \textit{para } x \textit{ suficientemente grande}$$

donde $H_h = \sum\limits_{k=1}^{\infty} \frac{\log[h(k)]}{k^2}$.

A continuación estudiaremos los casos especiales $g(n) = \prod_{j=1}^{n}(j,n)$ y $f(n) = g(n)^{\frac{1}{n}}$, y los comportamientos asintóticos y series de Dirichlet de $\log[g(n)]$ y $\log[f(n)]$. Empecemos por dar algunas cotas para la función $f(n)$.

Teorema 3.8. *La función f satisface las desigualdades*

$$max(n^{\frac{1}{\upsilon(n)}}, n^{\frac{\tau(n)}{2n}}) \leq f(n) \leq 27\left(\frac{\log(n)}{\omega(n)}\right)^{\omega(n)},$$

donde n es un entero positivo, $\omega(n)$ es el número de primos distintos que dividen a n, $\tau(n)$ es el número de divisores de n y $\upsilon(n)$ es el primo de mayor potencia que es divisor de n.

Demostración. Para la cota superior, el teorema 1.13 nos muestra que

$$\frac{\sum_{j=1}^{n}(j,n)}{n} \leq 27\left(\frac{\log(n)}{\omega(n)}\right)^{\omega(n)},$$

y usando la media aritmética-geométrica tenemos que

$$f(n) = \left(\prod_{j=1}^{n}(j,n)\right)^{\frac{1}{n}} \leq \frac{\sum_{j=1}^{n}(j,n)}{n},$$

de donde concluimos que

$$f(n) \leq \frac{\sum_{j=1}^{n}(j,n)}{n} \leq 27\left(\frac{\log(n)}{\omega(n)}\right)^{\omega(n)}.$$

Para la primera parte de la cota inferior tengamos en cuenta lo siguiente

$$\frac{1-p^{-\alpha}}{p-1} = \frac{p^{\alpha}-1}{p^{\alpha}(p-1)} > \frac{1}{p^{\alpha}}(p^{\alpha-1}+p^{\alpha-2}+...+p+1) \geq \frac{\alpha}{p^{\alpha}}.$$

Entonces tenemos

$$f(n) = \prod_{p^{\alpha}\|n} p^{\frac{1-p^{-\alpha}}{p-1}} \geq \prod_{p^{\alpha}\|n} p^{\frac{\alpha}{p^{\alpha}}} \geq \prod_{p^{\alpha}\|n} p^{\frac{\alpha}{\upsilon(n)}} = n^{\frac{1}{\upsilon(n)}}.$$

Para la segunda parte de la cota inferior tenemos

$$\left(\prod_{d|n} d\right)^2 = \left(\prod_{d|n} d\right)\left(\prod_{e|n} e\right) = \left(\prod_{d|n} d\right)\left(\prod_{d|n} \frac{n}{d}\right)$$
$$= \prod_{d|n} d\frac{n}{d} = \prod_{d|n} n = n^{\tau(n)}.$$

Finalmente, tenemos

$$f(n) = \left(\prod_{j=1}^{n}(j,n)\right)^{\frac{1}{n}} \geq \left(\prod_{d|n} d\right)^{\frac{1}{n}} = n^{\frac{\tau(n)}{2n}}.$$

■

Corolario 3.9. *La función g satisface las siguientes desigualdades*

$$n \leq max(n^{\frac{n}{\upsilon(n)}}, n^{\frac{\tau(n)}{2}}) \leq g(n) \leq 27\left(\frac{\log(n)}{\omega(n)}\right)^{n\omega(n)},$$

$g(n) = n$ si y solo si n es primo. Por lo tanto, para todo $\epsilon > 0$, tenemos

$$\log[g(n)] = O(n^{1+\epsilon}) \quad \textit{para } n \textit{ suficientemente grande.}$$

Demostración. Este corolario sigue de los teoremas anteriores. Si n es compuesto, entonces $\prod_{j=1}^{n}(j,n) > n$ donde $(n,n) = n$ y $(j,n) > 1$ por lo menos para un valor j menor que n. ■

Si hacemos $h(x) := x$ en (3.1) la serie de Dirichlet para $\log[g(n)]$ es

$$G(s) = \sum_{n=1}^{\infty} \frac{\log[g(n)]}{n^s}.$$

Para estudiar su convergencia hacemos $h(x) := x$ en el Teorema 3.1 y obtenemos

$$\begin{aligned} G(s) = \left(\frac{\zeta(s-1)}{\zeta(s)}\right) H_h &= \left(\frac{\zeta(s-1)}{\zeta(s)}\right)\left(\sum_{n=1}^{\infty} \frac{\log(n)}{n^s}\right) \\ &= -\frac{\zeta(s-1)\zeta'(s)}{\zeta(s)}, \end{aligned}$$

ya que $H_h = \sum_{n=1}^{\infty} \frac{\log(n)}{n^s} = -\zeta'(s)$.
Esto lo consignamos en el siguiente corolario

Corolario 3.10. *La serie de Dirichlet $G(s)$ converge absolutamente para $Re(s) > 2$ hacia*

$$-\frac{\zeta(s-1)\zeta'(s)}{\zeta(s)}.$$

Observemos que para

$$\sum_{n=1}^{\infty} \frac{\log[f(n)]}{n^s} = \sum_{n=1}^{\infty} \frac{\log[g(n)^{\frac{1}{n}}]}{n^s} = G(s+1).$$

Por último, estudiaremos los comportamientos asintóticos para los casos $\sum_{n\le x} \log[g(n)]$ y $\sum_{n\le x} \log[f(n)]$.

Teorema 3.11. *Tenemos las siguientes relaciones asintóticas*

$$\sum_{n\le x} \log[g(n)] = -\frac{\zeta'(2)}{2\zeta(2)}x^2 + O(x\log^3(x)) \quad \textit{para } x \textit{ suficientemente grande y}$$

$$\sum_{n\le x} \log[f(n)] = -\frac{\zeta'(2)}{\zeta(2)}x + O(\log^3(x)) \quad \textit{para } x \textit{ suficientemente grande.}$$

Demostración. Para la primera relación usamos el teorema 3.6 con $e(x) = x$ y tenemos que $H_e = \sum_{k=1}^{\infty} \frac{\log(k)}{k^2} = -\zeta'(2)$. Donde concluimos que

$$\sum_{n\leq x} \log[g(n)] = -\frac{\zeta'(2)}{2\zeta(2)}x^2 + O(x\log^3(x)) \quad \textit{para } x \textit{ suficientemente grande.}$$

Para el caso $f(n) = g(n)^{\frac{1}{n}}$, tenemos que

$$\log[f(n)] = \frac{1}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right)\log(d) = \sum_{d|n} \frac{\phi(\frac{n}{d})}{n/d}\frac{\log(d)}{d}.$$

Entonces para un x suficientemente grande tenemos

$$\begin{aligned}\sum_{n\leq x} \log[f(n)] &= \sum_{n\leq x}\sum_{d|n} \frac{\log(d)}{d}\frac{\phi(\frac{n}{d})}{n/d} = \sum_{d\leq x}\frac{\log(d)}{d}\sum_{e\leq \frac{x}{d}}\frac{\phi(e)}{e} \\ &= \sum_{d\leq x}\frac{\log(d)}{d}\Phi_1\left(\frac{x}{d}\right).\end{aligned}$$

Usando la estimativa Φ_1 (1.8), tenemos

$$\sum_{n\leq x} \log[f(n)] = \frac{x}{\zeta(2)}\sum_{d\leq x}\frac{\log(d)}{d^2} + \underbrace{O\left(\sum_{d\leq x}\frac{\log(d)}{d}\log\left(\frac{x}{d}\right)\right)}_{(1)}. \tag{3.6}$$

Utilizando la misma técnica del teorema 3.6, obtenemos

$$\frac{x}{\zeta(2)}\sum_{d\leq x}\frac{\log(d)}{d^2} = -\frac{x\zeta'(2)}{\zeta(2)} + O(\log(x)).$$

Usando el lema 3.5, el error (1) en (3.6) se convierte en

$$\begin{aligned}\sum_{d\leq x}\frac{\log(d)}{d}\log\left(\frac{x}{d}\right) &= O\left(\sum_{d\leq x}\frac{\log(d)}{d}\frac{\log^2(x)}{4\log(d)}\right) \\ &= O\left(\log^2(x)\sum_{d\leq x}\frac{1}{d}\right) \\ &= O(\log^3(x)).\end{aligned}$$

Por lo tanto,

$$\sum_{n\leq x} \log[f(n)] = -\frac{x\zeta'(2)}{\zeta(2)} + O(\log(x)) + O(\log^3(x))$$

$$= -\frac{x\zeta'(2)}{\zeta(2)} + O(\log^3(x))$$

■

Si escribimos el teorema anterior como

$$\log\left(\prod_{n\leq x} g(n)\right) = -\frac{\zeta'(2)}{2\zeta(2)}x^2 + O(x\log^3(x)) \quad \textit{para } x \textit{ suficientemente grande,}$$

entonces

$$\prod_{n\leq x} g(n) = e^{-\frac{\zeta'(2)}{2\zeta(2)}x^2}\underbrace{e^{O(x\log^3(x))}}_{1}.$$

Simplificando el error (1) en la anterior expresión tenemos que si

$f(x) = O(x\log^3(x))$, entonces existe $M > 0$ tal que $|f(x)| \leq Mx\log^3(x))$, luego

$$e^{|f(x)|} \leq e^{Mx\log^3(x))} = x^{Mx\log^2 x}.$$

Por lo tanto

$$\prod_{n\leq x} g(n) = O(x^{x\log^2(x)})e^{-\frac{\zeta'(2)}{2\zeta(2)}x^2} \quad \textit{para } x \textit{ suficientemente grande.}$$

Análogamente, al escribir $\sum_{n\leq x}\log[f(n)]$ en el teorema anterior tenemos

$$\prod_{n\leq x} f(n) = O(x^{\log^2(x)})e^{-\frac{\zeta'(2)}{2\zeta(2)}x} \quad \textit{para } x \textit{ suficientemente grande.}$$

Conclusiones que consignamos en el siguiente corolario.

Corolario 3.12.

$$\prod_{n\leq x} g(n) = O(x^{x\log^2(x)})e^{-\frac{\zeta'(2)}{2\zeta(2)}x^2} \quad \textit{para } x \textit{ suficientemente grande, y}$$

$$\prod_{n\leq x} f(n) = O(x^{\log^2(x)})e^{-\frac{\zeta'(2)}{2\zeta(2)}x} \quad \textit{para } x \textit{ suficientemente grande.}$$

Capítulo 4

Aplicaciones de la función $g(n)$

En este capítulo mostraremos algunas aplicaciones de la función $g(n)$.

a) Una de estas está relacionada con el número de soluciones distintas de la congruencia $x^{n-1} \equiv 1\,(mod\,n)$.

   Para un entero positivo n, el número de soluciones distintas módulo n de la congruencia $x^{n-1} \equiv 1\,(mod\,n)$ está dado por la formula

$$\prod_{p|n}(n-1, p-1).$$

   Una demostración de esta formula se dio en el teorema 1.16.

   Notemos que si $n = p$, p primo, el número de soluciones distintas módulo p de la congruencia

$$x^{\phi(p)} \equiv 1\,(mod\,p) \tag{4.1}$$

   es $p - 1$.

   En otro contexto esas soluciones son enteros para los cuales n es un seudo-primo.

Para un entero n compuesto impar, el número de enteros b con $1 \leq b \leq n$ y $(b,n) = 1$ tales que n sea un $Sp(b)$ es

$$B_{sp}(n) = \prod_{p|n}(n-1, p-1)$$

donde $B_{sp}(n)$ indica la cantidad de enteros b para los cuales n es un seudo-primo.

De igual forma que 4.1 notemos que si n es primo

$$B_{sp}(n) = p - 1$$

lo cual coincide con $\phi(p)$.

Si n es un número compuesto impar, tal que $n = p_1 p_2 ... p_k$, donde los p_i son primos, entonces

$$B_{sp}(n) = \prod_{p|n}(n-1, p-1) = \prod_{p|n} p - 1 = \phi(n).$$

b) Otra aplicación surge del estudio de los puntos reticulares sobre rectas en el plano.

Dados dos puntos reticulares $P(a,b)$ y $Q(c,d)$, el número de puntos reticulares que hay en el segmento $\overline{PQ}$ está dado por

$$(a-c, b-d) + 1.$$

Si P y Q son puntos cualesquiera en el plano, entonces el número de puntos reticulares que hay en el segmento $\overline{PQ}$ está dado por

$$([a-c], [b-d]) + 1.$$

Donde $[a-c]$ es la parte entera de $a-c$ y $[b-d]$ es la parte entera $b-d$.

Para el caso particular $y = \pm x$, para cualquier par de puntos $P(a,a)$ y $Q(b,b)$, el número de puntos reticulares del segmento $\overline{PQ}$ esta dado por

$[b-a]+1$.

Ahora bien,la función $g(n)$ aparece al obtener el número total de caminos que hay entre cada punto reticular de un segmento de recta a los demás puntos reticulares de diferentes segmentos de recta. Consideremos el siguiente ejemplo.

Dados los puntos en el plano $P(a_1,b_1)$; $Q(c_1,d_1)$ y $R(a_2,b_2)$; $S(c_2,d_2)$, el número de caminos que hay entre los puntos reticulares del segmento $\overline{PQ}$ y los puntos reticulares del segmento $\overline{RS}$ esta dado por el producto

$$[(a_1-c_1,b_1-d_1)+1]\times[(a_2-c_2,b_2-d_2)+1].$$

Si al ejemplo anterior le adicionados otro segmento $\overline{TU}$ formado por los puntos $T(a_3,b_3)$; $U(c_3,d_3)$ el número de caminos posibles esta dado por

$$\begin{aligned}&[(a_1-c_1,b_1-d_1)+1]\times[(a_2-c_2,b_2-d_2)+1]\\&+[(a_1-c_1,b_1-d_1)+1]\times[(a_3-c_3,b_3-d_3)+1]\\&+[(a_2-c_2,b_2-d_2)+1]\times[(a_3-c_3,b_3-d_3)+1].\end{aligned}$$

Bibliografía

[1] Andrew D. Loveless. *The General gcd-product function*, Integer:Journal of Combinatorial Number Theory, Vol 6 (2006), No 19.

[2] Andrew D. Loveless. *Corrgendum to:the General gcd-product function*, Integer:Journal of Combinatorial Number Theory, Vol 6 (2006), No 39.

[3] Apostol, T.M. *Introduction to Analytic Number Theory.* New York, Berlin Heidelberg: Springer-Verlag, 1976.

[4] K.A. Broughan. *The gcd-sum function*, Journal of Integer Sequences, Vol. 4 (2001), Article 01.2.2.

[5] E. Cohen *Arithmetical functions of greatest common divisor. I*, Proc. Amer. Math. Soc. 11 (1960).

[6] E. Cohen. *Arithmetical functions of greatest common divisor. II, An alternative approach*, Boll. Un. Mat. Ital. (3) 17, (1962), 329-356.

[7] E. Cohen . *Arithmetical functions of greatest common divisor. III. Cesáro's divisor problem*, Proc. Glasgow Math. Assoc. 5 (1961), 67-75.

[8] R. Baillie, S.S. Wagstaff, Jr., *Lucas Pseudoprimes*, Math. Comp. 35 (1980), 152, 1391-1417.

[9] A.D. Loveless, *A Compositeness Test that Never Fails for Carmichael Numbers*, Math. of Comp., preprint.

[10] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Great Britain: Cambridge University Press, 1995.

[11] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the theory of Numbers* , Fifth Edition. 1991.

[12] S.C. Coutinho, *Numeros Inteiros e criptografia RSA*, Segunda Edição, Serie de computação e Matemática. Instituto Nacional de Matemática Pura y Aplicada, IMPA.

[13] Van Der Poorten. *A proof that Euler missed: Apéry's proof of the irrationality of* $\zeta(3)$ *an informal report*, Centre for Number Theory Rescarch, Macquaric Universite, Sydney, 1979.

[14] Van Der Poorten. *Una demostración que se le escapó a Euler: la demostración dada por Apéry de la irracionalidad de zeta*(3)*, un informe informal*, Lecturas Matemáticas, Volumen 7, 1986.

[15] Balanzario Eugenio P. *Método elemental para la evaluación de la función zeta de Riemann en los enteros pares*, Instituto de Matemáticas, UNAM-Morelia. 2001.